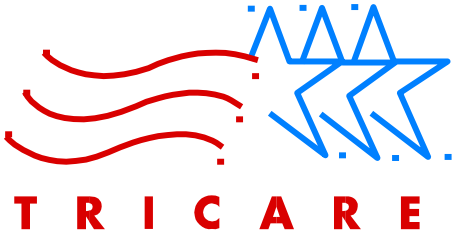
HEALTH AFFAIRS



TRICARE Management Activity

Military Health System (MHS) Information Assurance (IA) Architecture Framework

HEALTH AFFAIRS

MHS IA Architecture Framework

TRICARE Management Activity

Today's Environment

- Highly interactive environment devices and interconnected systems
- MHS routinely interacts with industry, private citizens, and other government agencies
- Complexity of today's systems and networks present great security challenges

HEALTH AFFAIRS

MHS IA Architecture Framework

TRICARE Management Activity

Legislative and Policy Drivers:

- Public Law 107-347 (Title III)
  Federal Information Security Management Act of 2002
- OMB Circular A-130 (Appendix III)
  Security of Federal Automated Information Resources
- DoD 8500.1
  Information Assurance (IA)
- DoDI 8500.2
  Information Assurance (IA) Implementation
- DoD 5200.40
  DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

HEALTH AFFAIRS

MHS IA Architecture Framework

TRICARE Management Activity

Challenges:

- Clinger-Cohen and OMB A-130 states that Enterprise Frameworks and Architectures (EAs) are to be used to manage IT and IT investments
  - IA not effectively included in Frameworks and EAs
  - IA not well integrated into system architectures or designs

HEALTH AFFAIRS

MHS IA Architecture Framework

TRICARE Management Activity

IA/Security Architecture:

- Identifies policies, standards, and security technologies necessary to protect information assets
- Objective of IA architecture is to ensure IA principles of:
  - Confidentiality – degree to which sensitive information requires protection from unauthorized disclosure
  - Integrity – degree to which sensitive information must be protected from unauthorized, unanticipated, or unintentional modification
  - Availability – degree to which sensitive information must be available on a timely basis to meet operational requirements or to avoid compromising

HEALTH AFFAIRS

MHS IA Architecture Framework

TRICARE Management Activity

IA/Security Architecture (continued)

- Authentication/ID – security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information
- Non-repudiation – assurance the sender of data is provided proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data

- Security architecture must document and respond to IA policies

HEALTH AFFAIRS

MHS IA Architecture Framework

TRICARE Management Activity

Applying IA to EA:

OMB Cir A-130		IA Principles		Security Services
Business Processes		Integrity		Authentication
Information Flows		Confidentiality		Accountability
Data Descriptions	+	Availability	+	Data Integrity & Non-repudiation
Applications		Authentication/ID		Confidentiality
Technology Infrastructure		Non-repudiation		Certification
				Security Management

TRM* SP

* TRM – Technical Reference Model
SP – Standards Profile

HEALTH AFFAIRS

MHS IA Architecture Framework

TRICARE Management Activity

Goals:

- Enhance ability to address IA in Enterprise Frameworks and Architectures
  - IA is increasing concern to all customers
  - All customers building or using frameworks
    - Federal Enterprise Architecture Framework (FEAF)
    - DoD Architecture Framework

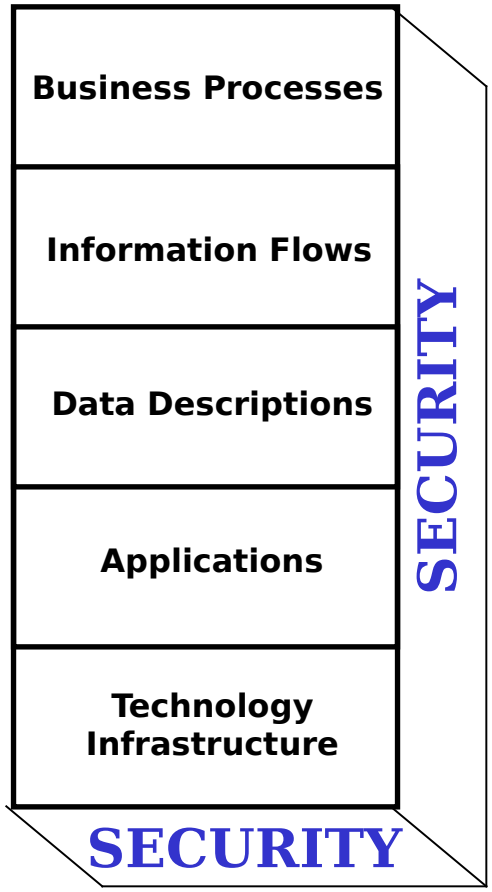
HEALTH AFFAIRS

MHS IA Architecture Framework

TRICARE Management Activity

MHS IA Architecture:

… a Framework



Backup Slides

HEALTH AFFAIRS

MHS IA Architecture Framework

TRICARE Management Activity

Information Security Framework